http://dx.doi.org/10.7236/JIWIT.2012.12.6.83
JIWIT 2012-6-10

AES 암호 알고리듬 기반 보안성이 강화된 RFID 인증 프로토콜 설계

Design of Security-Enhanced RFID Authentication Protocol Based on AES Cipher Algorithm

강민섭*

Min-Sup Kang

요 약 본 논문에서는 RFID 시스템에서 개인 정보보호를 위해 보안성이 강화된 인증 프로토콜의 설계를 제안한다. 제안된 방법에서는 AES(Advanced Encryption Standard) 암호 알고리듬을 기반으로 하여 3중 CRA(challenge response authentication) 방식을 사용한다. 또한, 개선된 인증 메카니즘의 실현을 위해 기존의 ISO/IEC 18000-3 표준을 수정한 3종류의 프로토콜 프레임 패킷 형식을 제안한다. 보안성 비교를 통하여 제안한 알고리듬이 보다 보안성이 강인함을 제시하였으며, 제안한 프로토콜의 검증을 위해 RFID Tag을 위한 디지털 Codec을 설계하였다. 설계된 Codec은 Verilog HDL을 사용하였고, Xilinx Virtex XCV400E device를 사용하여 합성을 수행하였다. 시뮬레이션 결과를 통하여 제안한 프로토콜이 안정성 향상과 함께 정확히 동작함을 보였다.

Abstract This paper proposes the design of a security-enhanced RFID authentication protocol which meets the privacy protection for tag bearers. The protocol which uses AES(Advanced Encryption Standard) cipher algorithm is based on a three-way challenge response authentication scheme. In addition, three different types of protocol packet formats are also presented by extending the ISO/IEC 18000-3 standard for realizing the security-enhanced authentication mechanism in RFID system environment. Through the comparison of security, it was shown that the proposed scheme has better performance in user data confidentiality, Man-in-the-middle replay attack, and replay attack, and forgery resistance, compared with conventional some protocols. In order to validate the proposed protocol, a digital Codec of RFID tag is also designed based on the protocol. This Codec has been described in Verilog HDL and also synthesized using Xilinx Virtex XCV400E device.

Key Words : Authentication protocol, AES cipher algorithm, RFID system, Verilog HDL

Ⅰ. Introduction

Radio Frequency Identification System (RFID) is the latest technology to play an important role for object identification as a ubiquitous infrastructure[1][2]. The tags attached to products are used to identify the object during production or in uses via radio frequency which may be passive or active[2].

*정회원, 안양대학교 컴퓨터공학과
접수일자 : 2012년 7월 23일, 수정완료 : 2012년 8월 23일
게재확정일자 : 2012년 12월 14일

Received: 23 July 2012 / Revised: 23 August 2012 / Accepted: 14 December 2012
*Corresponding Author: mskang@anyang.ac.kr
Dept. of Compter Engineering, Anyang University, Korea

The ISO/IEC 18000 standard defines a protocol for RFID tags that handles bi-directional communication between a reader device and the tags[2][3]. Unfortunately, the data exchange between RFID reader and tags on this protocol is not secure, and there are no mechanisms defined to authenticate the tags to the reader. When this protocol is used for the challenge-response process, it is vulnerable to a man-in-the-middle attack which is an eavesdropper can capture texts for both challenge and response by just sniffing with a protocol analyzer[4]. Thus, a cipher algorithm such as AES is necessary to protect branded goods from forgery.

In reference [5], a robust mutual fits the low-cost system in authentication protocol environment to meet the privacy protection for tag bearers. However, this approach is has not given any results implemented in hardware. In addition, the existing protocol which is defined in the ISO/IEC 18000-3 standard does not include cryptographic authentication mechanism[3].

This paper proposes the design of a security-enhanced RFID authentication protocol based on AES (Advanced Encryption Standard) cipher algorithm. In addition, three different types of protocol frame formats are also presented by extending the ISO/IEC 18000-3 standard[3] for realizing the proposed authentication mechanism in RFID system environment. In order to validate the proposed protocol, a digital Codec of RFID tag is also designed based on the proposed protocol.

II. Related Works

1. RFID system

RFID system is used for the automated identification of products, which is similar to smart cards. In this system, data can be stores and processed on a chip. In general, RFID systems are composed of three components such as RFID reader, RFID tag, and back-end server.

RFID reader includes antenna, transceiver and decoder which communicate with the tag, and it is also used as an interface between a back-end server and the tag. The RF tag which is placed on the object to be identified contains a transponder with a memory chip that possesses a unique ID. The back-end server which is secure server has a database which stores the various information of each tags obtained from the reader in some useful manner. In general, Thursted Third Party (TTP) can read all messages, and if TTP is compromised, all communications are insecure.

The various command signals (queries) are generated in the reader, and the signals can be received in a tag when a tag is within range of the signal. The tag sends out its identification (anonymous ID) or encoded data to the reader, when responding to commands from the reader. The received ID then should send to the back-end server to be processed.

Fig. 1 shows the configuration of RFID system for implementing security-enhanced authentication protocol based on AES cipher algorithm which will be presented in this paper.

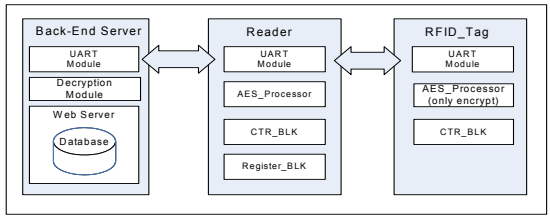

Fig 1. Configuration of RFID system
그림 1. RFID 시스템의 구성도

2. Authentication protocol

A Hash Lock scheme which was presented by MIT[2] based on a hash function. The reader has key k for each tag, and each tag holds the result metaID, metaID = hash(k) of a hash function. The reader sends a key that is related to metaID received from the tag, and a tag receives a request for ID access and sends metaID in response. The tag then calculates the hash function from the received key and checks whether the result of the hash function corresponds to the metaID

stored in the tag. Although this scheme offers good reliability at low cost, since metaID is fixed, the adversary can track the tag via metaID.

To resolve this problem, Randomized hash lock scheme has been introduced by MIT, which is an extension of the hash lock type scheme[2]. It requires the tag to have a hash function and a pseudo-random generator. Each tag calculates the hash function based on the input from pseudo-random generated, r and id, i.e., c = Hash(id ‖ r). The tag then sends c and r to the reader.

The reader sends the data to the back-end server. The server calculates the hash function using the input as the received r and id for each ID stored in the server. The server then identifies the id that is related to the received and sends the id to the reader. The tag output changes with each access, so this scheme deters tracking.

However, this scheme allows the location history of the tag to be traced if the secret information in the tag is revealed, i.e., this scheme cannot satisfy the forward security requirement.

Thus, on the basis of AES cipher algorithm, a new security-enhanced authentication protocol will be presented for RFID system in this paper.

Ⅲ. Proposed Authentication Algorithm

1. Security-enhanced authentication protocol

The protocol is the technical framework on which all future products can be built, including tags, readers and other technology[9]. Conventional randomized hash lock scheme allows the location history of the tag to be traced if the secret information in the tag is revealed. The enhanced protocol is designed on the basis of the concept of "the reader talks first" [7]. This means that any tag does not start transmitting unless it has received and properly decoded an instruction sent by the reader.

Fig. 2 shows the proposed security-enhanced authentication protocol for RFID system based on AES algorithm.

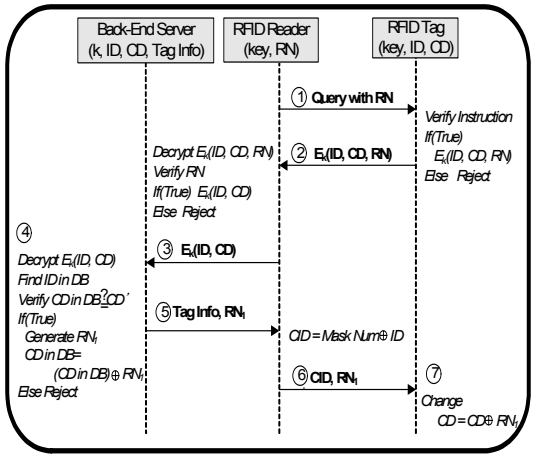

Fig 2. The proposed security-enhanced authentication protocol based on AES algorithm

그림 2. AES 알고리듬에 기반한 보안성 향상을 위해 제안된 알고리듬

This protocol which uses AES (Advanced Encryption Standard) cipher algorithm is based on a three-way challenge response scheme which is an exchange of a request from reader to tag and a response from the tag to the reader. In this approach, the random number is generated by the reader while the conventional approach generates it in the tag[2]. Thus, our scheme can be realized low-cost tag by reducing hardware-overhead of the tag compare to the conventional one.

In this work, back-end Server is that host computer has database (DB) including tag information such as ID (chip serial numbers of tags), k (key value of tags), and each data. We assume that both the server and tags have unique secret key of k, and Reader has Random Number Generator (RNG) which generates random number denoted as RN.

Now, we explain the detailed procedure for executing the proposed authentication protocol.

In (Step 1), Reader sends a query with RN as challenge to Tag. We defined this query to an extended

Inventory request packet (EIQP) in which RN is inserted (see Table 1), which is extension of the original Inventory request format defined in ISO/IEC 1800-3[3].

In (Step 2), Tag generates an encrypted data, E_k(ID, CD, RN) using AES algorithm, and the data is inserted into an extended Inventory response packet (EIPP) shown in Table 2, which is extension of the original Inventory response packet. Then, Tag sends the packet as response to Reader. Note that the encrypted data() is used for protecting the man-in-the-middle-attack since the encrypted data are useless to an attackers.

In (Step 3) Reader decrypts the received data, E_k(ID, CD, RN) from Tag, and obtains RN′. If the decrypted RN′ and RN are identical, this proves the authenticity of Reader. Next, both ID and CD are encrypted using secret key, k; E_k(ID, CD), and then Reader sends E_k(ID, CD) to Back-end server

In (Step 4), Back-end server decrypts Ek(ID, CD) and obtains both ID and CD′ which are the corresponding decrypted values. Using this ID, if the corresponding CD in database (DB) has found, CD is compared with CD′. If both values are identical, this condition proves the authenticity of Tag. If authentication process is successfully terminated in this step, then CD is changed by Exclusive-OR operation of CD and RN1, i.e., CD = CD ⊕ RN1, where RN1 is a random number generated by RNG. Thus, CD can be used to prevent replay attack to the used tag once. In (Step 5), only the Server sends data (Tag Info and RN1) to Reader.

In (Step 6), Reader generates first CID by Exclusive-OR operation of Masking value (Mv) and ID, i.e., CID = Mv ⊕ ID, and then Reader reconstructs an EIQP packet using the both CID and RN1. In this time, Reader sends this new packet to Tag, which is shown in Table 3.

In (Step 7), Tag ID is extracted from the received CID from Reader using Masking value, and then CD is changed; CD = CD ⊕ RN1. The data obtained in this Step are used to make the encrypted data such as E_k(ID, CD, RN) for next communication. As a result, replay attack in this Tag can be prevented because the original value CD is changed by Exclusive-Oring with RN1.

2. Design of extended protocol packets

The ISO/IEC 18000-3 standard describes the communication of the tags with a reader using a frequency of 13.56Mhz[3][5]. For communication between two units, the reader sends a Request data to the tag, and receives a Response data from the tag. Request and Response are contained within a frame with Start-of-Frame (SOF) and End-of-Frame (EOF) the delimiters. In general, General Request format consists of SOF, Flag, Command Code, Parameters, Data, CRC and EOF.

In Command code, four types of commands are defined: Mandatory, Optional, Custom, and Proprietary. In the proposed authentication mechanism, two kinds of command are used: Inventory and Select commands defined in Mandatory and Optional to communicate with two units. Table 1 shows an example of an EIQP format with a random number, RN which modifies standard Inventory request format.

Table 1. An extended Inventory request format with RN

표 1. RN을 가진 확장된 Inventory 요청 형식

SOF	Flags	Invent.	Opt. AFI	Mask length	Mask-value	RN	CRC	EOF
	8bits	8bits	8bits	8bits	0-64bits	16bits	16bits	

The standard Inventory response contains the fields of Flags, DSFID, UID, and CRC[3]. In the extended version shown in Table 2, two fields of CD and RN are added to the packet assigned to each 16 bits.

In Table 2, E_k(AES Encryption) means that six fields of Flags, DSFID, UID, CD, RN and CRC are the encrypted data. E_k(ID, CD, RN) using AES algorithm is used to identify the Tag sending the response. Thus, the extended Inventory response packet is used to provide location privacy and to protect the

man-in-the- middle-attack since the encrypted data are useless to an attackers.

Table 2. An extended Inventory response format with CD and RN
표 2. CD와 RN을 가진 확장된 Inventory 응답 형식

SOF	Ek(AES Encryption) ="0xD3E2F30ADE47D80D03808B99DF00580"						EOF
	Flags	DSFID	UID	CD	RN	CRC	
	8bits	8bits	64bits	16bits	16bits	16bits	

The standard Select request contains the fields of Flags, Select, UID, and CRC. In the extended version, UID field is changed to CID and RN1 field with16 bits is added to the packet. Table 3 shows an extended Select request packet (ESQP) format with CID and RN1, which modifies conventional standard Select request format.

Table 3. An extended Select request format with RN1
표 3. RN1을 가진 확장된 Select 응답 형식

SOF	Flags	Select	CID	RN1	CRC	EOF
	8bits	8bits	64bits	16bits	16bits	

As we can see from the proposed protocol shown in Fig. 2, the original value CD is changed by Exclusive-Oring with RN1 after CID is verified. Thus replay attack can be prevented by using this modified packet.

The proposed protocol has been evaluated the view point of the security requirement. Table 4 shows the comparison of the security requirements and the possible attacks. Data items for comparison make reference to results shown in [5].

Table 4. Comparison between some protocols
표 4. 제안한 프로토콜과의 성능비교

Protocols	HLS [5]	EHLS [5]	HBVI [7]	Proposed	
User data confidentiality	X	△	△	O	Step 1
Forgery Resistance	X	X	X	O	Step 1
Mutual authentication	△	△	△	O	Steps 1,3
Man-in-the-middle attack prevention	△	△	X	O	Step 2
Reader authentication	X	X	X	O	Step 3
Tag anonymity	X	△	△	O	Step 5
Replay attack prevention	△	△	O	O	Step 7

† Notation
O : Satisfied, △ : Partially satisfied, X : Not satisfied

IV. Digital Codec Design and Simulation

The RFID system is divided into two parts of analog front-end and digital parts. The analog front-end part is responsible for modulation and demodulation of data for the power supply of the tag and the digital part(Codec) handles control functions and data processing tasks[4].

The digital Codec for a Tag is composed of Packet Processor, CRC(Cycle Redundancy Check) Calculator, System Controller, AES cipher algorithm, and EPROM. AES(Advanced Encryption Standard) is a symmetric key encryption technique, which provides strong encryption.

Packet-processor filters the required data after analyzing commands of various packets received from RF/analog front-end. It is possible for reconstruction of the packed data which will be sent to the reader. CRC calculator block calculates CRC value on data for transmitting and receiving and it compares the CRC value with the received one for detecting errors during transmission[4]. It is also read some information from tag memory, EPROM. The EPROM has been stored in unique information of tag's ID, CD and key value of k.

The Codec designed has been described in Verilog HDL, and logic synthesis has been performed using Xilinx Virtex XCV400E device which is supported by IDEC of KAIST in Korea.

In order to verify operation of the system, initial

vectors for EPROM in this Tag are required, which have three fields of UID, DSFID and key value of k; UID = 0x686B0A07000007E0, CD = 0x8ADE, AES Key(Ek) =0x2B28AB097EAEF7CF15D2154F16A6883C[8].

In addition, three types of the packet data are used as input vectors for simulation, which is given in Table 1, 2 and 3. A packet data shown in Table 1 is used as input vector for simulating the extended Inventory request format. Two packets of Table 2 and 3 are also used as input vectors for the EIPP and the EIQP formats, respectively. In order to fully validate the designed Codec, the timing simulation has been also performed using Mentor Graphics' ModelSimTM.

Fig. 3 shows the process for generating an EIPP in Tag after CRC verification is finished. Packet data fields for encryption in Tag are Flags, DSFID, UID, CD, RN, and CRC which is consisted of "0000686b0a07000007e08adeabcd48d7" as shown in ellipse of Fig. 3.

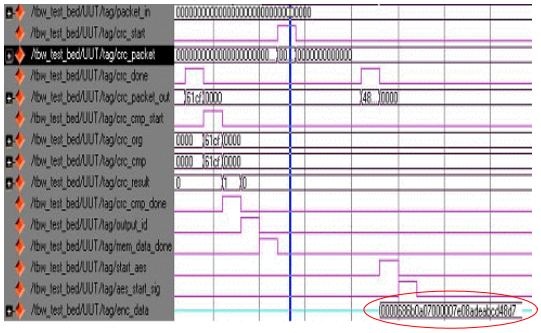

Fig 3. Process for generating EIPP in Tag
그림 3. Tag에서 EIPP 을 생성하는 과정

As described In Step 3 of our algorithm, Reader should be decrypt the received data, Ek(UID, CD, RN) from Tag, and then the decrypted data is "0xD3E2F30ADE47D80D03808B99DF00580" shown in Table 2. Fig. 4 shows process for selecting Tag from data generated in Reader, where The received data is "2325e2b5f5f8fffff81fef120000e8b5" which is the part shown in the rectangle of Fig. 4 (see Table 3).

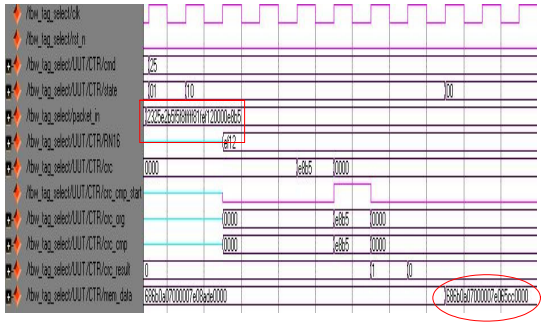

Fig 4. Process for selecting Tag
그림 4. Tag를 Select하는 과정

In this time, Tag verifies both data of CRC and CID, and then CD is changed with new value, i.e. CD = CD ⊕ RN1 (ef12). Output data (mem_data) is composed of both UID and CD, and this data is stored in memory of Tag which is a part shown in ellipse.

V. Conclusions

In this paper, the design of a security-enhanced RFID authentication protocol has been presented based on AES encrytion algorithm, which meets the privacy protection for tag bearers. In addition, digital Codec for RFID tag has been designed based on the protocol.

The designed Codec is described in Verilog HDL and synthesized using the Synopsys Design Compiler. The proposed security-enhanced protocol has better performance in user data confidentiality, tag anonymity, Man-in-the-middle attack prevention, replay attack, and forgery resistance, compared with some protocols[5][7].

References

[1] M. Jakobsson and D. Pointcheval, "Mutual Authentication for Low-power Mobile Devices," Lecture Notes in Computer Science, pp. 178-195, 2002

[2] Stephen A. Weis, Sanjay E.Sarma, Ronald L. Rivest

and Daiel W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", First International Conference on Security in Pervasive Computing, 2003

[3] International Organization for Standardization, "ISO/IEC 18000-3, Information Technology AIDC Techniques - RFID for Item Management," March 2003

[4] Martin Feldhofer, "A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags," IEEE Proceedings of MELECON 2004, Vol. 2, pp. 759-762, 2004

[5] J. Yang, K. Ren, and K. Kim, "Security and Privacy on Authentication Protocol for Low-cost RFID," Proceedings of SCIS2005, Jan., pp. 25-28, 2005

[6] D. Eastlake and P. Jones, "US Secure Hash Algorithm 1 (SHA-1)," Internet RFC 3174, September 2001

[7] Weis, S., Sarma, S., Rivest, R., and Engels, D., "Security and Privacy Aspects of Low-Cost RFIDs," Security in Pervasive Computing, Lecture Notes in Computer Science, Vol. 2802, pp. 201-212, 2003

[8] Joan Daemen, Vincent Rijmen, "AES Proposal : Rijndael",(http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf)

[9] Hae-Jung Kim, Eun-jun Yoon, and Jongjung Woo, "Cryptanalysis and Improvement of an RFID Authentication Protocol Based on Private Codes, Journal of KIIT, Vol. 9, No. 5, pp. 103-110, 2011

저자 소개

Min-Sup Kang

- 1979 : BS degree in Department of Telecommunication Engineering, Kwangwoon University.
- 1984 : MS degree in Department of Electronic Engineering, Hanyang University
- 1992 : PhD degree in Department of Electronic Engineering, Osaka University
- 1984 ~ 1992 : Senior researcher, ETRI(Electronics and Telecommunications Research Institute)
- 2001 ~ 2002 : Visiting scholar in Department of electrical & computer Engineering, University of California, Irvine
- 1993 ~ present : Professor, Department of Computer Engineering, Anyang University

<Research interests : ASIC design, imbedded system, cipher processor design, network security, RFID/USN>